ORIGINAL

ROBERT T. HASLAM (Bar No. 071134)
ROBERT B. HAWK (Bar No. 118054)
ROBERT D. FRAM (Bar No. 126750)
HELLER EHRMAN WHITE & McAULIFFE
525 University Avenue, Suite 1100
Palo Alto, California 94301-1900
Telephone: (415) 324-7000

JAMES R. BUSSELLE (Bar No. 75980)
TOMLINSON ZISKO MOROSOLI & MASER
200 Page Mill Road, Second Floor
Palo Alto, California 94306
Telephone: (415) 325-8666

Attorneys for Plaintiff, Counterclaim-Defendant, and Counterclaimant
RSA DATA SECURITY, INC.

231

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

C-94-20512-SW.

RSA DATA SECURITY, INC., a Delaware corporation,

Plaintiff,

v.

CYLINK CORPORATION, a California corporation, CARO-KANN CORPORATION, a California corporation, and THE BOARD OF TRUSTEES OF THE LELAND STANFORD JUNIOR UNIVERSITY, a California corporation,

Defendants.

AND RELATED COUNTERCLAIMS.

Case No. ~~C96-20094-SW~~

RSA DATA SECURITY, INC.'S POST-*MARKMAN* HEARING BRIEF

The Hon. Spencer Williams

TABLE OF CONTENTS

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES (Cont.)

TABLE OF AUTHORITIES (Cont.)

INTRODUCTION

This brief replies to Defendants' Response to RSADSI's Amended Proposed Jury Instructions and RSADSI's Memorandum In Support Thereof, filed after the close of the stipulated briefing schedule prior to the hearing. Basic fairness requires that RSA be permitted to respond to the points made by Defendants and to address the evidence offered at the hearing itself.

Defendants' position on claim construction distills to an attempt to persuade the Court not to limit the claims of the '582 patent to the embodiment disclosed in the specification (and its equivalents) -- a trapdoor knapsack cryptosystem. They do this by eschewing any reference to the specification. Defendants then turn around, however, and borrow aspects of those same embodiments (those related to limiting the invention to use on a digital computer) from the specification where necessary to save the claims from invalidity under § 101.

Defendants' attempt selectively to pick and choose those aspects of the specification that bolster their position while hoping to evade those limitations that injure their case is guided by no principle other than Defendants' self-interest. By contrast, RSA urges the Court to give them what they actually invented. In the '582 Patent, the inventors described what they posited was a *workable* public key cryptosystem. They represented to the Patent Office that their system, unlike those in the prior art, was workable. And their system was workable only because they had invented a trapdoor knapsack cryptosystem.

There are two accepted claim construction doctrines which lead the Court to construe these claims properly so that they encompass the inventors' true invention. First, the Court may limit the asserted claims of the '582 patent to the embodiments disclosed in the specification or their equivalents pursuant to 35 U.S.C. § 112 ¶ 6. Such a construction is consistent not only with longstanding precedent, it is also consistent with the inventors' election to draft their claims in broad functional terms, thereby subjecting them to the requirements of the statute. Alternatively, the Court may simply, and properly, construe certain claim elements by reference to the specification.

I. CLAIMS 1-6 OF THE '582 PATENT ARE MEANS- OR STEP-PLUS-FUNCTION CLAIMS WHICH MUST BE CONSTRUED AS LIMITED TO THE TRAPDOOR KNAPSACK AND ITS EQUIVALENTS UNDER § 112 ¶ 6.

Section § 112 ¶ 6 represents a compromise. In 1946, the Supreme Court rejected claims written in purely functional language for indefiniteness and overbreadth. *Halliburton Oil Well Cementing Co. v. Walker*, 329 U.S. 1 (1946). Congress then enacted what is now § 112 ¶ 6 expressly to permit such functional claim language, but only on the condition that the scope of the claims so written would be limited to the disclosed embodiment and its equivalents.[1/] In so doing, Congress struck a balance: § 112 ¶ 6 permits

---

1/ Section 112 ¶6 provides:

> An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

inventors the freedom to draft their claims using functional language, but prevents inventors from patenting the future by limiting the scope of their claims to that which the inventor actually invented.

With respect to claims 1-5, Defendants now contend that these claims are not step-plus-function claims at all. The Court must therefore determine whether these claims, as drafted and as allowed by the Patent Office, are in fact subject to § 112 ¶ 6.[2/]

With respect to claim 6, Defendants agree that this claim is subject to § 112 ¶ 6 and is limited to the structures disclosed in the specification and their equivalents, if any. Defendants, however, argue that the disclosed structures are just the individual generic circuit elements themselves, and not the structures made up of those circuit elements configured to perform the particular operations set forth in the specification. There is no fair reading of the specification that supports Defendants' attempt to read Messrs.' Hellman and Merkle's basic invention -- the trapdoor knapsack -- out of the claim.

A. CLAIMS 1-5 ARE FUNCTIONAL CLAIMS SUBJECT TO THE LIMITATIONS OF § 112 ¶ 6.

Claims 1-5 of the '582 Patent are step-plus-function claims because their elements are expressed as steps for performing a function without the inclusion of any acts in support thereof. 35 U.S.C. § 112 ¶ 6. Moreover, these claims contain terms of art,

---

2/ The applicability of § 112 ¶ 6 to claims 1-5 of the '582 Patent has been briefed in the Federal Circuit as part of Defendants' appeal of the denial of the preliminary injunction. The argument will likely be held in December.

"steps" and "such that," which, when used with purely functional language, typically render a claim subject to § 112 ¶ 6. *See Greenberg v. Ethicon Endo-Surgery, Inc.*, 91 F.3d 1580, 1583 (Fed. Cir. 1996); *Raytheon Co. v. Roper Corp.*, 724 F.2d 951, 957 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 835 (1984).

In the third element of claims 1, 4, and 5, the step of generating the secret key is described by its function: "such that the secret key is directly related to and computationally infeasible to generate from the public key." Ex. 13, '582 Patent at 19:5-8; 19:42-44; 19:68-20:2. Likewise, in the fifth element of claim 1, the step of enciphering the message is set forth in functional terms: "such that the enciphering transformation is easy to effect but computationally infeasible to invert without the secret deciphering key." Ex. 13, '582 Patent at 19:13-16; *see also id.* at 19:48-50; 20:6-8.

These elements do exactly what the Supreme Court prohibited in *Halliburton* and what Congress later allowed only subject to the limitations of § 112 ¶ 6; they use functional language at the point of novelty. Instead of telling one skilled in the art *how* to generate such a secret key and public key or *how* to encipher a message so that it is infeasible to decipher, they merely state certain general attributes that must apply to the relationship of these two keys or to the relationship of the enciphering and deciphering transformations. Such functional claim language is indefinite and overbroad unless limited to the specific embodiment and its equivalents. *See Genentech Inc. v. Wellcome Foundation, Ltd.*, 29 F.3d 1555, 1570 (Fed. Cir. 1994) (Lourie, J.

concurring). To learn *how* to implement a workable public key system -- which is the only point of novelty of the '582 invention -- one must look to the discussion of the trapdoor knapsack cryptosystem in the specification.

The prosecution history affirms this construction by revealing that this functional language represents the exact point of novelty of the '582 invention. Two prior art articles, *Multiuser Cryptographic Techniques* and *New Directions in Cryptography*, described the necessary attributes of the secret key and of the enciphering transformation. *See* Ex. 1001, Whitfield Diffie and Martin Hellman, *Multiuser Cryptographic Techniques*, 45 AFIPS Conf. Procs. 109, 110 (June 8, 1976); Ex. 1000, Whitfield Diffie and Martin Hellman, *New Directions in Cryptography*, II-22 IEEE Transactions on Information Theory 644, 648 (Nov. 1976). As the inventors twice emphasized in response to the Examiner's rejections, the prior art articles failed to provide a "workable" algorithm for generating such a secret key or performing such an enciphering transformation. *See* Ex. 16, '582 Prosecution History, Amendment at 19 (Feb. 13, 1979); *Id.*, Amendment at 10 (Oct. 4, 1979); *see also* Ex. 13, '582 Patent at 2:38-47.

The novel aspects of the invention of the '582 Patent are, therefore, *how* to generate a secret key that is directly related to and computationally infeasible to generate from the public key and *how* to encipher a message so that it is computationally infeasible to decipher it without the private key. These points of novelty, however, are only described in purely functional terms in the claim language of the '582 patent. In

other words, the inventors' "workable" algorithm -- the trapdoor knapsack cryptosystem -- is found in the specification, not in the claim language. In such circumstances, the claim must be construed pursuant to § 112 ¶ 6. *See In re Roberts*, 470 F.2d 1399, 1402 (C.C.P.A. 1973); *Laitram Corp. v. Rexnord, Inc.*, 939 F.2d 1533, 1536 (Fed. Cir. 1991).

The expert testimony of Dr. Konheim also confirms that claims 1-5 must be construed subject to the limitations of § 112 ¶ 6. Dr. Konheim testified that the third element of claim 1, "generating from said random numbers a secret deciphering key at the receiver," does not have a well-understood meaning in the art of cryptography because it describes the result of a process but not how to do it. Hearing Tr. at 62:4-15; *cf. Greenberg*, 91 F.3d at 1583. In other words, Dr. Konheim, as one skilled in the art of cryptography, regards that claim element as purely functional, without supporting acts described in the claim itself.

Defendants raise three arguments that despite the claim language, the prosecution history, and the expert testimony, claims 1-5 should be construed as method claims not subject to § 112 ¶ 6: (1) the inventors did not opt to invoke § 112 ¶ 6; (2) because claim 6 is clearly subject to § 112 ¶ 6, claims 1-5 cannot be; and (3) courts have failed to apply § 112 ¶ 6 to other claims containing the terms "steps" or "such that." For the reasons set forth below, none of these arguments has merit.

1. The Inventors of the '582 Patent Opted to Invoke § 112 ¶ 6 by Drafting Claims 1-5 In Purely Functional Language.

Defendants argue that in the absence of either the words "steps for" in the claims themselves or an explicit statement in the prosecution history, the Court should presume that the inventors did not intend to invoke § 112 ¶ 6 and therefore that provision does not apply to claims 1-5. Defendants, however, mischaracterize the "option" that § 112 ¶ 6 presents an inventor. Contrary to Defendants' suggestion, the Patent Act does not permit an inventor to choose between (1) using the term "steps for" and having the claims limited to the disclosed embodiment and its equivalents, or (2) not using the terms "steps for" and having the claims construed to include every possible act that achieves the claimed result. Indeed, if Defendants' formulation of the choice were correct, § 112 ¶ 6 would have no meaning because any means- or step-plus-function claim could be rewritten without the "magic" language, thereby avoiding the provision's limitations on functional claims.

As the plain language of § 112 ¶ 6, as well as its history and purpose, makes clear, the statute offers an inventor the choice of using functional language provided that the claims so drafted are limited in scope.[3/] An inventor may either (1) draft claims using broad functional language without supporting acts which are limited to the disclosed embodiment and its equivalents,

---

3/ The choice, moreover, was made during prosecution. Defendants' argument that application of §112 is something they can waive today, Hearing Tr. 266:12-15, or may decline at their option, *Id. at 265:25, ignores the rule that patentees may "rewrite [their] patent claims to suit [their] needs in this litigation." Mason v. Tampa G. Mfg. Co.*, 1995 WL 605556 at **4 (Fed. Cir.) (citing *Nike, Inc. v. Wolverine World Wide, Inc.*, 43 F.3d 644, 647 (Fed. Cir. 1994)).

or (2) draft claims which contain specific acts and therefore are not purely functional. The inventor cannot have it both ways.

Here, the plain language of claims 1-5 demonstrates that the inventors of the '582 opted to describe their invention in broad functional language without including supporting acts. Unless their scope is limited to the disclosed trapdoor knapsack systems and their equivalents, these claims are no different from the invalidly overbroad claims of *Halliburton*. Thus, claims 1-5 should be construed subject to the limitations required by § 112 ¶ 6.

2. The Fact That Claim 6 Is Drafted in Means-Plus-Function Form Supports the Conclusion that Claims 1-5 Are Also Subject to § 112 ¶ 6.

Citing the aid to claim construction of claim differentiation, Defendants argue that because claim 6 is subject to § 112 ¶ 6, claim 1 cannot be. To the contrary, in this case, the similarities between claims 1-5 and claim 6 suggest that all six claims should be construed according to § 112 ¶ 6.

The principle of claim differentiation cited by Defendants plainly does not aid in the analysis of claims 1 and 6. Since claim 1 is a method claim and claim 6 is an apparatus claim, they need not be further differentiated. In other words, because construing both claims 1 and 6 subject to § 112 ¶ 6 would not render either claim "superfluous," no presumption arises that they must be construed differently in this respect.[4/] *See Tandon Corp.*

4/ Nor does the fact that claims 7-17 specifically claim the trapdoor knapsack cryptosystem prevent claims 1-6, as means- or step-plus-function claims "from being interpreted as statutorily mandated by section 112(6)." *Laitram Corp. v. Rexnord, Inc.*, 939 F.2d 1533, 1538 (Fed. Cir. 1991).

v. United States Int'l Trade Comm'n, 831 F.2d 1017, 1023 (Fed. Cir. 1987). Patentees commonly draft a pair of claims, including a method claim and a "means for" apparatus claim, both of which contain essentially the same elements. *See, e.g., Laitram Corp. v. NEC Corp.*, 62 F.3d 1388, 1389-90 (Fed. Cir. 1995); *Arrhythmia Research Technology, Inc. v. Corazonix Corp.*, 958 F.2d at 1053, 1055 (Fed. Cir. 1992); *Bio-Rad Laboratories, Inc. v. Nicolet Instrument Corp.*, 739 F.2d 604, 608 (Fed. Cir.), *cert. denied*, 469 U.S. 1038 (1984); *BOC Group, Inc. v. Novametrix Medical Systems, Inc.*, 11 U.S.P.Q.2d 1853, 1857 (D. Conn. 1989), *rev'd on other grounds*, 15 U.S.P.Q.2d 1475 (1990). In analyzing such claim pairs, courts have discussed § 112 ¶ 6 with regard to neither claim, *see Laitram Corp. v. NEC Corp.*, 62 F.3d at 1394-95; *Bio-Rad*, 739 F.2d at 609-10, 613-14, both claims, *see BOC Group*, 11 U.S.P.Q.2d at 1857-59, or only the "means for" apparatus claim, *see Arrhythmia*, 958 F.2d at 1060; courts typically perform basically the same analysis, however, in construing both claims. Nowhere does the Federal Circuit indicate that the fact that § 112 ¶ 6 has been raised in the context of an apparatus claim but not a method claim mean that it is never appropriate to apply § 112 ¶ 6 to method claims simply because the section also applies to an apparatus claim.

Contrary to Defendants' contention, the Federal Circuit's decision in *Arrhythmia* does not suggest that the Court should interpret method claim 1 of the '582 patent without reference to § 112 ¶ 6 just because an apparatus claim in the patent (claim 6) is written in "means plus function" language. While it is true that

the Federal Circuit did not mention § 112 ¶ 6 when analyzing the method claim in *Arrhythmia*, the simple fact is that the Court was not asked to do so by any of the litigants. Moreover, there were two strong reasons why the court did not need to consider § 112 ¶ 6 in the context of that case.

First, the Court in *Arrhythmia* determined to construe the method claim in light of the specification, even without resort to § 112 ¶ 6. Thus Defendants' assertion that "the Court analyzed the claimed method steps of 'converting,' 'applying,' determining,' and 'comparing' without reference to any acts from the specification" is plainly incorrect. Defs.' Markman Brief at 20:3-5. The Federal Circuit, in fact, interpreted these method claim elements according to the description in the specification. For example, the court interpreted the third element, "determining an arithmetic value of the amplitude of the output of said filter" as follows: "The filtered signal is further analyzed to determine its average magnitude, as described in the specification, by the root mean square technique." *Id.* at 1055, 1059. In other words, the court looked to the embodiment disclosed in the specification to learn *how* to determine the arithmetic value.

Second, unlike the broad functional claims at issue here, the Federal Circuit in *Arrhythmia* carefully distinguished the method claim at issue in that case from invalidly overbroad claims such as those at issue in *O'Reilly v. Morse*, 56 U.S. 62, 113 (1854). Unlike Morse's improper attempt to patent the future by claiming any use of electric current to transmit characters at a distance, the claims in *Arrhythmia* "do not encompass subject matter

transcending what [the inventor] invented." 958 F.2d at 1059. In contrast, each of the first six claims of the '582 Patent is as broad as Morse's invalid claim. Thus, claims 1-5, like claim 6, must be limited to the trapdoor knapsack and its equivalents pursuant to § 112 ¶ 6.

3. Claims 1-5 Not Only Contain Designating Terms Such As "Step" or "Such That" But Also Are Written In Purely Functional Language, Requiring the Application of § 112 ¶ 6.

The general rule, recently set forth in *Greenberg*, that claims should be interpreted subject to § 112 ¶ 6 where the term "means for" or "steps for" or something in the prosecution history suggests that the inventor elected to invoke § 112 ¶ 6, is not absolute.[5/] 91 F.3d at 1584. Moreover, where, as here, the claim is written in functional terms, and where such functional language is designated by the words "so that" or "such that", the *Greenberg* court itself observed that the claims fall within § 112 ¶ 6.

Attached to Defendants' Markman reply brief are two appendices listing claims containing the terms "steps," "steps of," "such that" or "so that" to which the Federal Circuit did not apply § 112 ¶ 6. Defendants ask rhetorically: why, when the claims in all ten of these cases contain the same designating terms as claims 1-5 of the '582 Patent, did the court fail to consider the applicability of § 112 ¶ 6?

The simple answer is that § 112 ¶ 6 was not raised in any of these cases and so the court was not *asked* to consider its

---

5/ Nor do Defendants dispute the fact that there are exceptions to the *Greenberg* rule. *See* Defs.' Markman Br. at 13 n.4; Defs.' Markman Reply Br. at 4:5.

applicability. In addition, a closer look at the cases in the appendices reveals that there is ample reason why none of them explicitly considers and rejects the application of § 112 ¶ 6. In some cases the consideration of § 112 ¶ 6 is clearly unnecessary, such as when the meaning of the claim element containing the designating term is not disputed by the parties, *see, e.g., Bell Communications Research v. Vitalink Communications Corp.*, 55 F.3d 615, 618 (Fed. Cir. 1995) ("defining a spanning tree on said graph such that every pair of said nodes is connected by only one of said paths...") or when the patent is invalid under another provision. *See, e.g., In re Warmerdam*, 33 F.3d 1354, 1360 (Fed. Cir. 1994) (finding claims 1 and 2, which contain the terms "steps of" and "step of," respectively, invalid under § 101 as non-statutory subject matter).

In other cases, the claim language at issue is clearly not the type of purely functional language without supporting acts that renders a claim subject to § 112 ¶ 6. Even if a claim contains the term "steps" in the preamble, if it also states specific acts for performing those steps, § 112 ¶ 6 does not apply. *See, e.g., Northern Telecom, Inc. v. Datapoint Corp.*, 908 F.2d 931, 934 (Fed. Cir.) *cert. denied*, 498 U.S. 920 (1990) ("connecting selected input/output peripheral components including at least a keyboard data entry means .... to a buffer memory and to a central processor organization, and using said buffer memory for temporary storage of data entered by said keyboard means"); *Standard Havens Products, Inc. v. Gencor Indus., Inc.*, 953 F.2d 1360, 1365 (Fed. Cir. 1991) *cert. denied*, 506 U.S. 817 (1992) ("isolating a zone of

said rotating drum from said hot gas stream"). Likewise the terms "so that" or "such that" do not necessarily introduce purely functional language, but rather may introduce descriptive language that has a precise meaning for those of skill in the art. *See, e.g., Kalman v. Berlyn Corp.*, 914 F.2d 1473, 1475 (Fed. Cir. 1990) ("introducing a filter . . . so that a part of the filter extends across said passage").

In contrast to the claims in the appendices, claims 1-5 of the '582 Patent not only contain the designating terms "steps" and "such that" but they are also extremely general and many elements set forth a result without specifying how to achieve it. Without the limitations imposed by Congress as a condition for using such functional language, these claims would be excessively broad. Thus, the Court should construe claims 1-5 as subject to § 112 ¶ 6.

B. CLAIM 6 MUST BE CONSTRUED TO COVER CIRCUIT ELEMENTS CONFIGURED TO PERFORM THE OPERATIONS OF THE TRAPDOOR KNAPSACK ALGORITHM AND ITS EQUIVALENTS.

Defendants do not dispute the fact that claim 6 is a means-plus-function claim, which, under § 112 ¶ 6, must "be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof." 35 U.S.C. § 112 ¶ 6. Defendants, though, now inexplicably maintain that the "corresponding structures" are just the circuit components depicted in the figures of the specification. In other words, according to Defendants, claim 6 should be construed to cover the circuit elements depicted in the specification, but not in the

configuration in which they appear in the specification: the trapdoor knapsack cryptosystem.

Pursuant to § 112 ¶ 6, the patentee may claim a means for performing a function but, at the same time, the patentee "must describe in the patent specification some structure which performs the specified function." *Valmont Industries, Inc. v. Reinke Mfg. Co., Inc.*, 983 F.2d 1039, 1042 (Fed. Cir. 1993); *see also Arrhythmia*, 958 F.2d at 1060 (construing a means-plus-function element as follows: "The high pass filter means is described in the specification as the minicomputer *configured* to perform the function of reverse time order filtration of the anterior portion of the QRS waveform") (emphasis added).

As is clear from the specification and as Mr. Dusse's unrebutted testimony confirms, the structures described in the specification are circuit elements configured to perform a particular function: the trapdoor knapsack cryptosystem. *See* Hearing Tr. at 126:6-22. For example, Mr. Dusse testified that the structure depicted in Figure 11 is a key generator. This structure is composed of circuit elements and it performs the key generation function in the second embodiment as described in the specification. Hearing Tr. at 127:3-10. According to Mr. Dusse, those circuit elements are not interchangeable parts; rather, they are configured specifically to perform the mathematics of the knapsack algorithms. Hearing Tr. at 127:11-128:17.[6/]

6/ Perhaps the clearest example of the difference between the parties positions is exemplified by looking at Figures 4 and 6 of the patent. The adder and subtractor depicted in Figures 4 and 6, respectively, "have roughly the same number and type of gates" and (continued...)

Defendants' current position is inconsistent with their Supplemental Responses to RSA's First Set of Interrogatories. There, Defendants effectively acknowledged that the structures disclosed in the specification of the '582 patent were configured to execute the trapdoor knapsack cryptosystem. *See* Ex. 1005, Response to Interrogatory No. 4 and Appendix B. Those responses make clear that the descriptions in the specification (as well as the figures) encompass the circuit elements disclosed in the specification only as configured in a particular way: they are configured to execute the computation of the trapdoor knapsack cryptosystem. *See, e.g.*, Ex. 13, '582 Patent at 12:33-16:23.

In sum, claim 6 must be limited to the circuit elements configured as described in the specification. It is therefore limited to circuit elements configured to perform the operations of the trapdoor knapsack algorithms or their equivalents, if any.

II. CLAIMS 1-5 MUST BE CONSTRUED AS LIMITED TO WHAT THE INVENTORS ACTUALLY INVENTED -- A TRAPDOOR KNAPSACK CRYPTOSYSTEM.

Apart from the specific statutory limitation of § 112 ¶ 6, there is Federal Circuit precedent for narrowing broad claims such as claims 1-5 of the '582 patent. Where, as here, the novel invention *is* that which is disclosed in the specification, the

---

6/(...continued)
yet perform very different functions "based largely on the different connections that are made between those gates." Hearing Tr. at 126:16-22. Those are, therefore, very different structures. Defendants, however, would argue that they are essentially the same because made up of the same elements. Defendants are driven to this position because of the arguments they want to make on infringement: their position is tantamount to saying that a pancake is the same as a loaf of bread because each is made with flour, milk and eggs.

specification properly guides and limits the construction of the claims. *See Modine Mfg. Co. v. United States Int'l Trade Comm'n*, 75 F.3d 1545, 1551 (Fed. Cir.), *cert. denied*, 116 S. Ct. 2523 (1996). Like the patentee in *Modine*, the inventors of the '582 Patent limited their claims during prosecution. As discussed above, the inventors twice amended their claims to distinguish the prior art by representing to the Patent Office that their invention was a workable public key system. *See* Ex. 16, '582 Prosecution History, Amendment at 19 (Feb. 13, 1979); *Id.*, Amendment at 10 (Oct. 4, 1979). In fact, that which the inventors invented, a "workable" trapdoor knapsack cryptosystem, is found only in the specification.

Moreover, where the claims, if broadly construed, are abstract, mathematical concepts which are unpatentable under § 101, the claims are properly limited to "what the claimed steps do" as described in the specification. *See Arrhythmia*, 958 F.2d at 1059. For example, the court, in construing the claim element, "determining an arithmetic value of the amplitude of the output of said filter," did not turn to the dictionary to define the term "determining", as Defendants urge in this case. Rather, the court looked to the specification where this step is accomplished "by the root mean square technique." *Id.* The court validated the claims as construed by reference to the specification because it could answer the question: "What did the applicant invent?" Here,

likewise, if the Court asks what the inventors of the '582 Patent invented, the answer must be a trapdoor knapsack cryptosystem.[7/]

III. THE COURT MUST NOT ADOPT DEFENDANTS' PROPOSED DEFINITIONS THAT SELECTIVELY IMPORT LIMITATIONS FROM THE SPECIFICATION OR EXTRINSIC SOURCES IN ORDER TO PRESERVE THE VALIDITY OF THE CLAIMS.

Both in their briefs and in their argument, Defendants urged the Court to consider intrinsic evidence above all else and insisted that the Court may not read limitations into the claims, no matter how great the temptation. Defs.' Markman Br. at 4-10; Defs. Markman Reply Br. at 8; Hearing Tr. at 8:23-11:15. Defendants cautioned the Court that it must determine the validity of these claims on another day. Defs.' Markman Br. at 10-11; Defs.' Markman Reply Br. at 12-13; Hearing Tr. at 256:7-18. The definitions of certain terms proposed by Defendants, however, are flatly inconsistent with these oft-repeated assertions.

With their proposed definitions of certain claim terms, Defendants are again trying to have it all. On the one hand, they advocate the broadest possible construction of claims 1-6 so as to encompass all of public key cryptography. On the other hand, Defendants subtly transform claims 1-6 from the abstract algorithms described in the claims into processes described only in the

---

7/ To the extent there is any lingering ambiguity concerning the proper scope of claims 1-5, Federal Circuit precedent favors the narrower interpretation and construes the disputed claim only as broadly as its unambiguous scope. *See Athletic Alternatives, Inc., v. Prince Mfg., Inc.*, 73 F.3d 1573, 1581 (Fed. Cir. 1996); *Ethicon Endo-Surgery, Inc. v. United States Surgical Corp.*, 93 F.3d 1572, 1581 (Fed. Cir. 1996). Therefore, consistent with Federal Circuit precedent, claims 1-5 should be construed to cover the trapdoor knapsack cryptosystems disclosed in the specification.

specification that manipulate the physical world. This they do in an attempt to save the claims from invalidity under § 101.[8/]

Defendants have improperly introduced physical elements, such as computers and digital signals, into the claim language. They do so by reference to extrinsic "last resort" sources. Despite the fact that the functions described could be performed using a computer, the plain claim language nowhere requires it.

1. Message: Defendants' definition of message concludes: "Usually in cryptographic communications, such messages are transmitted as a series of zeroes and ones." Defs.' Amended Proposed Jury Instruction No. 3 ¶1. In fact, only when cryptographic communications are transmitted digitally need they be transmitted as a series of zeroes and ones.[9/] Claims 1-5 are broad enough to read on a pencil and paper implementation of a public key cryptosystem.

2. Processing: Defendants' definition concludes: "In the context of a digital signal processor, processing is the act of

---

8/ Mere mathematical constructs are not patentable subject matter, *see Warmerdam*, 33 F.3d at 1360. Moreover, where there is no reference in the claim language itself to the transformation of physical matter or digital signals by the mathematical concept in question, the claim is non-statutory under § 101. *See In re Schrader*, 22 F.3d 290, 294 (Fed. Cir. 1994); *In re Abele*, 684 F.2d 902, 907 (C.C.P.A. 1982). A thorough discussion of these issues is provided in RSA's Opposition to Defendants' Motion for Summary Judgment on the Validity of the '582 Patent, Section III, pages 29-35 and Appendix A.

9/ Neither of the technical dictionaries on which Defendants rely contain any suggestion that messages are generally transmitted as a series of zeroes and ones. *See* Ex. 500, McGraw-Hill Dictionary of Scientific and Technical Terms (3d ed.) at 1002; Penguin Dictionary of Computers at 300.

transforming digital signals or data or manipulating digital signals or data." Defs. Amended Proposed Jury Instruction No. 3 ¶9.[10/] Again, the literal claim language reads on non-digital implementations.

Defendants are understandably concerned about the abstract nature of the claims as they have sought to construe them, free of the confines of § 112 ¶ 6. Defendants boldly stated that they were willing adopt a reading of the claims based on the naked language itself. Having done so, Defendants should be required to sink or swim without the very sort of "lifeline" from the Court, grounded in extrinsic evidence, that they so strongly insist they do not need.

IV. SPECIFIC TERMS IN CLAIMS 1-6 SHOULD BE CONSTRUED CONSISTENTLY WITH THEIR USE IN THE SPECIFICATION AND BY THOSE SKILLED IN THE ART OF CRYPTOGRAPHY.

In addition to addressing the issues discussed, the Court will need to construe some other specific terms. The parties have proffered proposed jury instructions on these terms and have responded to each other's proposed instructions. Discussed below are three specific terms, "securely," "computationally infeasible," and "authentication," in light of the evidence presented at the *Markman* hearing.

A. SECURELY.

10/ In contrast, the dictionary definition that Defendants urge the Court to adopt defines the verb "process" as "to manipulate data or to act based on certain data" without requiring that the data be digital. *See* Ex. 507, Computer Professional's Dictionary at 268.

Claims 1, 2, 3, and 6 describe a method or apparatus for "communicating securely over an insecure communication channel." Although neither the claims nor the specification define the term "securely," it has a well-understood meaning in the art of cryptography. As Dr. Konheim testified, a "secure" cryptographic system is one which "guarantees to provide secrecy against any and all methods that people can bring to bear against the system . . . for at least some time." Hearing Tr. at 28:5-18. The Federal Circuit has held that it is appropriate for the Court to receive such "extrinsic evidence in order 'to aid the court in coming to a correct conclusion' as to the 'true meaning of the language employed' in the patent." *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 980 (Fed. Cir. 1995) (en banc) (quoting *Seymour v. Osbourne*, 78 U.S. 516, 546 (1871)), *aff'd*, 116 S. Ct. 1384 (1996).

"Security" in the context of cryptography may mean either unconditional security or computational security. *See* Hearing Tr. at 35:8-11. Dr. Konheim opined that the use of the term "securely" in the '582 Patent refers to a computationally secure system. Hearing Tr. at 54:12-55:7. Such a computationally secure system is only considered secure by those skilled in the art after it has withstood attack with current and future algorithms and resources for a reasonable period of time. *See* Hearing Tr. at 32:11-16, 47:5-10. Only after a system has proven itself secure against concerted attempts to break it is it informally certified by the cryptographic community.[11/] *See* Hearing Tr. at 40:9-20, 48:4-20.

11/ Defendants' proposed definition of "securely" -- "although in theory one may be able to break the security of the system, it is (continued...)

That the definition of "securely" given by Dr. Konheim is shared by those skilled in the art is confirmed (1) by articles by the inventors approximately contemporaneous with the filing of the patent application, *see* Ex. 1000, W. Diffie and M. Hellman, *New Directions in Cryptography* at 653; Ex. 1003, R. Merkle and M. Hellman, *Hiding Information and Signatures in Trapdoor Knapsacks* at 529; Ex. 1004, W. Diffie and M. Hellman, *Privacy and Authentication* at 399, (2) by the testimony of Cylink's expert in the MIT matter, Ex. 1006B, Washington Depo. at 201:22-202:9, and (3) by an authoritative treatise on cryptography, *see* Ex. 22, B. Schneier, *Applied Cryptography* at 7; Hearing Tr. 39:20-53:22.

B. COMPUTATIONALLY INFEASIBLE.

The third and fifth elements of claims 1,[12/] 4, 5, and 6 contain the term "computationally infeasible." These four claims describe a secret key that is "computationally infeasible" to generate from the public key and an enciphering transformation that is "computationally infeasible" to invert without the secret key.

The specification defines "computationally infeasible" as follows:

> A task is considered computationally infeasible if its cost as measured by either the amount of memory used or the computing time is finite but impossibly large, for example, on the order of approximately 10^{30} operations with existing computational methods and equipment.

11/(...continued)
thought to be infeasible to do so" -- thus slightly misses the mark. Defs.' Amended Proposed Jury Instruction No. 3 ¶2. A system is considered secure not just because it is thought to be infeasible to break it but because it has been shown, over a period of time, to be impervious to attack.

12/ Claims 2 and 3 are dependent on claim 1.

Ex. 13, '582 Patent at 5:10-14. The Federal Circuit has found that the specification "may act as a sort of dictionary." *Markman*, 52 F.3d at 979.

In this case, the specification dictionary defines "computationally infeasible" to mean having a "finite but impossibly large" cost, as measured in either time or memory. In other words, a task is computationally infeasible if it is impossible, as a practical matter, to complete it although in theory it can be done. Because a secure cryptosystem must both protect the secrecy of information and protect it over time, the cost to the eavesdropper (either as measured in time or in number of computers he would need) of discovering the information must be prohibitively high.[13/]

The computational infeasibility of generating the secret key from the public key or of inverting the enciphering transformation without the secret key is what makes the cryptosystem secure. Determining whether an operation is in fact computationally infeasible, therefore, requires subjecting the operation to attack over a period of time using both current and future resources. *See* Hearing Tr. at 58:25-59:6.

C. AUTHENTICATING.

Claims 2 and 3 contain the phrase "authenticating the receiver's identity." Dr. Konheim opined that in the art of

---

13/ The specification includes an example of 10^{30} operations with existing computational methods and equipment. Dr. Konheim estimated that with 1977 methods and equipment, 10^{30} operations would take 10^{16} years, which is "many, many lifetimes." Hearing Tr. at 60:15-61:5. The example simply underscores the enormous length of time that a task must take in order to be considered computationally infeasible.

cryptography "authenticating" means "verifying the identity of the receiver" or "finding some method of proof that you're dealing with the person who claims to be the receiver." Hearing Tr. at 70:5-16. His view is confirmed by the patent specification, Ex. 13, '582 Patent at 18:46-58, and by an article by the inventors, Ex. 1003, R. Merkle and M. Hellman, *Hiding Information and Signatures in Trapdoor Knapsacks* at 527.

Defendants assert that "[w]hen the patent claims refer to 'authenticating' someone's 'identity,' those terms do not necessarily require that the person's name, social security number or other identifier has been verified." Defs.' Amended Proposed Jury Instruction No. 3 ¶12. Defendants' definition finds no explicit support in the patent and, in fact, contradicts the description in the specification. The specification clearly describes the use of a public file so that a secret key may be linked with a particular person (by the showing of a driver's license, etc.) thereby allowing the person to authenticate his or her identity by the use of that secret key. Ex. 13, '582 Patent at 18:46-58. In light of the plain meaning of the term "authenticate", Defendants may not rewrite their patent claims to serve their present needs. *See Mason v. Tampa G. Mfg. Co.*, 1995 WL 605556 at **4 (Fed. Cir.)

Moreover, claim 2, read literally and without resort to the specification, does not add anything to claim 1. The receiver has already deciphered the message in the last step of claim 1, and therefore already has the ability to decipher the message. That ability to decipher, therefore, does not authenticate the

receiver's identity. Claim 2, therefore, must have hidden somewhere in its language some additional act. But the plain language of claim 2 does not tell one what that "something" is.

Claim 3 provides some insight, because claim 3 provides that the step of claim 2 "includes" sending a representation of the message. That means, of course, that the step of claim 2 also has something in addition to sending the representation of the message. *See Ethicon Endo-Surgery, Inc. v. United States Surgical Corp.*, 93 F.3d 1572, 1575 (Fed. Cir. 1996). Once again, however, the plain language of claim 2 does not provide any guidance on what those steps are. It is only by resort to the specification and the acts set forth therein, either under §112 ¶ 6 or by claim construction, can one construe claim 2 in any meaningful way.

CONCLUSION

This Court should (1) construe claims 1-5 as step-plus-function claims or as otherwise limited to the trapdoor knapsack invention;[14/] (2) construe claim 6 to cover the circuit elements configured as described in the specification; and (3) construe specific terms consistent with the plain language of the claims and the understanding of those terms in the art of cryptography.

DATED: October 24, 1996

HELLER EHRMAN WHITE & McAULIFFE

By: _____
Robert T. Haslam
Attorneys for Plaintiff,
Counterclaim-Defendant,
and Counterclaimant RSA DATA
SECURITY, INC.

14/ The parties are attempting to stipulate to which disclosures in the specification correspond to the steps in claims 1-5.